University of Rhode Island Cybersecurity Symposium Keynote Address

General Keith Alexander, Director of the National Security Agency and US CYBER COMMAND

April 11, 2011

You know, let me be real honest. Thank you for that great introduction, but the way the Army promotes people is alphabetically. I know that. (laughter) So let's be honest about this.

Two, it's an honor and privilege to be here. First, my hat's off to Congressman Langevin for what you've done for our country in cybersecurity. I know Senator Whitehouse has talked about this, but you know two things, when you look at it from my perspective. I think cybersecurity is one of the most important issues facing our nation today. Congressman Langevin led, co-founded the first ever Congressional Cybersecurity Caucus in 2008 and then co-chaired the CSIS Commission on Cybersecurity for the 44th President. Absolutely superb. Perhaps more importantly, he's looked at this, he's studied this, he's been a leader in the House and, Sir, thank you very much for what you do.

It's interesting that Rhode Island, not just the university, but your elected officials lead in this area. As Senator Whithouse, as you heard, he has tremendous depth as well. You would be very proud to know that you state leads in this area. And Senator Whitehouse thank you for what you've done. I know on the Senate Select Committee for Intelligence, you led that panel. You did a superb job. You are one of the few people that I've ever seen go in and really study and get to the ground too. So let's give them a big round of applause.

[Applause]

Ok, I've got to remember to push the advance button, I know this on these things here, so I'll try to remember that. But before I do, I brought with us, we also have at the National security agency, we have a graduate from the University of Rhode Island, I think in 1886. Am I off? December. It was December. Oh 1986. Steve please stand up. Steve Ryan.

Now the reason I had him stand up is he's one of the architects for cybersecurity at the National Security Agency and has led the development of defensive censors for our nation. Absolutely superb. You ought to be proud of one of your alumni. We are proud of you Steve, so thanks.

With that, I know I'm on a timeline here, not the movie, and I'll throw some jokes in, it's ok to laugh [laughter]. I get graded if they are funny.

First, cybersecurity. You heard what Senator Whitehouse said, tremendous opportunity in this space. Look at what's going on, many of you have the new iPhones, the iPads. These mobile devices. And when you look at the amount of mobile devices from 2000, we had about 500 million mobile phones, now about five billion out there. Just about everybody on the planet has

one. I guess several of you have many and some are without. But tremendous opportunities and look at what's going on and what this means to the future.

When you look at Deep Blue up in the upper left hand corner, and Watson in the lower right hand corner, look at what's going on in this area. We're going mobile. We're getting better capabilities, lots of applications. The opportunities are limitless. I believe that these capabilities will help us solve many of the problems we have with cancer, with other forms of disease, with how we collaborate in the future. It's the wave. It's coming. We have to be prepared for it.

And I'll tell you, this is something to look forward to. You've heard all the statistics, so let me jump to the next thing. It can also be used for social networking, for setting up some things like snowball fights on the Mall. Very important. It's not often you get snow on the Mall. But perhaps more importantly, look at what's happened in the Middle East when you look at Tunisia, Libya, Egypt, the use of social network forums for starting and changing leaders, a huge jump forward.

And if you think about it, you're starting to see some of those leaders look at, well how do we stop people from using these networks? So you're seeing people use them and others try to stop it and I think that's going to be part of our future.

So, what I want to talk briefly about on this slide here was to introduce the threat. I'll hit off some of the key comments that Senator Whitehouse had, but when we look at the threat, look at exploitation, that's been going on for years, but it doesn't mean it's right. But it has been going on and its getting worse. You heard the number $1 trillion. It comes from a McAfee report about the intellectual property and other forms of problems on the network, monetary problems that we face. Now I bring up intellectual property because that's what we're losing from foreign actors in these spaces for industry. Our government's been losing secrets. When we think about the companies that have been hit, Nasdaq, RSA, Google. Those are companies that you would think are at the top of cybersecurity and cyber defense. And if they get hit, where does put companies that are in the electrical sector and other sectors of our government? It's a huge problem.

If you shift that a little bit to the right and look at the middle: disruption. I had the privilege to go out to Estonia. It is a country. I can tell you that. I thought that perhaps the E was part of E-stonia and it was just a virtual place, but it's a real country. And I met with President Ilves. In fact we sat on a panel this weekend. They got hit in 2007, in Tallinn, the monument, the Soviet monument that was taken down. This was a diplomatic, political agenda. The Estonians were taking down that. The Russians didn't want that to go down. They were hit with a massive distributive denial of service attack.

Now that's a disruption, because that's like that one person who Senator Whitehouse said, 60,000 emails in 2 hours. They got hundreds of millions of emails into their system and it disrupted their ability to communicate, took down their banking sector. They had to close off all external communications outside the country. It impacted them significantly, caused them to jump towards now for NATO the lead for a cyber center of excellence and other things like that, but they weren't the only ones. You see under that, the little picture there of Georgia. It's hard to read perhaps for those in the back, but that's what that represents, that little fuzzy object there

which is when the Russians came into Georgia it was uniquely accompanied by a cyber attack on the Georgian infrastructure another disruptive attack.

And Latvia, Lithuania, Kyrgyzstan and Azerbaijan have also been hit by disruptive attacks. And those are attacks that disrupt, but once they stop you can clean it up and get back to work. What I'm concerned about are destructive attacks, those that are coming. And I've put down some unclassified examples to give you some insights to this, just to give you an idea of what could happen. And some of these were not attacks, but mistakes that have happened, but it gives you some insights.

The Northeast Power Grid problem in August of 2003 was based on software issues where a race condition was set up when three power lines, three high voltage power lines went down simultaneously, and what that did, it caused a race condition back to the central node and when it got all three at once, it went offline because that wasn't supposed to happen. And when it went offline, those inside the center assumed everything was ok, and when other lines started to go down, they didn't recognize the problem of power being drawn off. And when power started to get drawn off from other sectors, those quickly started to go down. It caused a cascade that shutdown the Northeast power section in four minutes and you know the problems from there.

The one shown on this slide is the Sayano-Shushenskaya dam, which is a dam in Russia and we probably should just call it the S-dam, but I thought well that wouldn't be appropriate in this audience, so I tried to pronounce it. This is the third largest in the world hydroelectric dam. What happened, there was a fire in Russian about five hundred miles away. There are ten huge hydroelectric turbines in this dam, each 640 megawatts. 640 megawatts. That's huge. And they needed one of these to come online when the other power system went off about 500 miles away, so they turned it on remotely. Well what they didn't realize is the sensing system that showed when things were going off kilter, when it started to spin, was offline. So they had no idea that this thing was going to go, start to wobble and break free of its infrastructure.

Now, why would that be a concern? Well first, those turbines weigh around 1500 tons. 1500 tons and pushing through it is about 75,000 gallons of water a second. Think of that as an Olympic pool. And so when this broke free it caused that turbine to raise up in the air about 50 feet and when it came back down, it destroyed the other nine, killed 75 people, and all done because somebody turned it on remotely and didn't have the ability to sense that there was a problem.

What I'm concerned about: these are issues that were caused by people with good intentions. What about those without? And there are two forms of the destruction that I'm concerned about. One is data, destroying data, and the other is equipment and I think we have to be ready for both of those.

2008: the Defense Department recognized that we had malicious software in our networks. And in our networks, we realized that this was brought to us by our own people, who used thumb drives to go from the unclassified networks to classified systems and when they did that, they brought this malicious software. We had a number of problems on that network. It was identified by the National Security Agency's Advance Network Ops Team. And when they recognized it, they were able to build a system in 22 hours to negate this, 22 hours. Oh, by the way, it always

happens on a Friday. All problems happen on a Friday, so they came in at 16:30 on a Friday and said here's the problem and they had the solution in by 14:30 on Saturday, they had it up and running. That's a huge, huge capability that our nation needs and I'll come back and talk about that in a minute.

So, that was the key issue that started the United States Cyber Command. And you know we're not in this alone. You see that we put in here US Cyber Command, the National Security Agency and Department of Homeland Security. It takes a team to operate in this space. What I wanted to talk about a little bit on this slide was what did we do? What did the Secretary of Defense do? We used to have our defense under the global network ops, the joint taskforce under DISA. The operate and defend were in one sector. The exploit and our offensive capabilities under NSA and our joint function component command for net warfare. What this meant is that we had different levels of classification. NSA operates at a top secret level. Our network defenders operate at a secret level. They could not know everything they we know. And when you think about it, that would be like telling your defensive team, you're only going to get a little bit of information. We have a lot more, but we can't share it with you. That's ludicrous. So what the Secretary did is he pushed both of those joint taskforces together and formed US Cyber Command.

Now I wanted to hit some key things that the President said in his May 29 speech because I think this is important to this audience and I want to get these exactly right because what he's put out here was huge for us and for our nation. And I think what you'll see, from my perspective, is this is the driving force, this was done on 29 May 2009. [Showing slide of Obama] I was going to actually have a cut out of me standing next to him, but some of you might have remembered the speech and I wasn't there so I thought, ok, so that probably wouldn't be right, but then you'd say, well he's cyberspace so...

Here's a few key things that he said in this. First, "cyberspace is real and so are the risks that come with it."

"The cyber threat is one of the most serious economic and national security challenges we face as a nation."

And finally, "protecting the digital infrastructure is a national priority."

So there's the President. This was the first speech done by a President on cybersecurity, pointing the vector ahead. Key to our economy, key to our national security and we've got to do something about it. And I think that's what Senator Whitehouse and Congressman Langevin are talking about and we appreciate that.

So let me take this the next step. Based on that, what our Deputy Secretary of Defense did, was wrote an article for the Foreign Affairs magazine. Now I don't want you to go back and read that necessarily. I just want to hit five key topics. I'm going to talk about two of those because those are key to what we need to do.

The first one was cyber as an operational domain analogous to air, land, sea and space. The two I'm going to talk about are the Active Defense, the second one there, and the third one, extending

that defense to critical infrastructure. Fourth, we do need partners: government within government as a team; between government and industry; and with our allies. And finally I'm going to end up on, we're the nation that built the internet, we're the nation that built most of the tools, we ought to be the leaders of securing that.

So let's talk about the active defense. If you look at how we defend our systems today, what we normally do is we have McAfee or Norton 360 and we put that up. And we tell our System Administrators, here you keep this up, you configure your network this way. It is very much a static capability. We'll upload new signatures but this is the way it happens. This is the way we do it. We depend on each of you to do it right. And then somebody will come up with a new zero-day exploit. They'll break into the system. They'll get a bunch of hooks into that system and they'll start taking data out.

After a while, sometimes 6-10 months, somebody says something's wrong here. We find this new exploit, we beat the system administrator [laugh], we patch the system. Now, if you're not a System Administrator, you're comfortable with this approach. [laughter]

This is analogous to the Maginot line. What we're doing is static. We have to do much more. We have to build that defense up. We have to have this go the full depth of what we can in cyberspace and do all of that. What would that entail? From my perspective that includes, an active capability inside your networks. Let's give the System Administrators an active role and train them to be advanced network operators looking for the threats. The system that Steve Ryan built, we call Tutelage. We've got to have a system that can communicate, with inside the system and outside the system to know when we have a problem between industry, our allies and our systems.

How do we give early warning in cyberspace? A new concept. But that's something that you would logically do and we should do it here. So we've got to build this out. We've got to have the capability to do that and we've got to be able to move seamlessly to ward off those threats.

So, when you think about that, that means that we have to have a partnership between the Defense Department and the Department of Homeland Security. In September 2010, Secretary Gates and Secretary Napolitano signed a memorandum of agreement that began that partnership, recognizing that we can't afford to build another National Security Agency, that we would need to leverage what NSA has, not only for US Cyber Command, but also for the Department of Homeland Security. I think that's a huge step forward.

The second issue that I wanted to talk about was extending this to the critical infrastructure. Today, and often times Members of Congress will ask me, so how are you going to defend the country in cyberspace? Well, right now that's not my mission. My mission as the Commander of US Cyber Command, is to defend the military networks. That's what authority I have today. I do not have the authority to look at what's going on in other government sectors nor what would happen to critical infrastructure. That right now falls to DHS.

It also means that I can't stop it, or in network speed, see what's happening to it. What we do believe though, is that needs to be accounted for. We have to have a way of protecting critical

infrastructure, like our power. And, when you look at it, if you were to ask me to rank order where industries are in terms of their cybersecurity capability, I think power is at or close to the bottom of the list, not because they're bad, but because that's not a focus area for them right now. Not only that, they don't have the technical expertise nor the government help that they need and we ought to give it to them. And so I think that partnership is going to be key for the future.

So, how do we extend this was one of the key things that Secretary Lynn talked about in that article and I think that's a huge issue for our country.

Now, when you think about it, one of the key things that comes up is about civil liberties and privacy and here's why being here today is so important to us. My opinion: civil liberties and privacy are not at the expense of cybersecurity. They will benefit from cybersecurity and we have to have a way of doing that. It means, from my perspective, accountability about what we're doing and oversight by Congress and by the Administration. Technically we can do that. We can do 100 percent audit and oversight and I think that's something the American people should demand and that we should provide.

On the other hand, it's not saying that, well, since we're concerned that NSA might touch that network, we can't secure it. I think the answer is, no, we can do both, and we should. So the question is how do we put those together?

You know, I think it's also important, I've been at NSA almost six years, and you say why so long? Well they have a rule I found out. It's that you stay there until you do something useful. So they said you may be there for a long, long time. A great bunch of people. One of the most technically proficient workforces I have ever seen. One of the key things that I got when I got up there was how they protect our civil liberties and privacy. Every member of our workforce is required to go through training on handling the US person's data and protecting it. And every time we take or make a mistake, we self report, to Congress and to the Administration. We take it very seriously.

We know what you're asking of us and what you're giving us to do in our intelligence roles is huge and that you demand and should demand that we have accountability in this area. And I will tell you it is my privilege and honor to supervise these people and be there leader because they do it better than anybody else. Absolutely superb.

I wanted to end on a couple things here. You know the four folks around the outside [on slide]: Bill Gates, Steve Jobs, Sergey Brin and Mark Zuckerburg. Key leaders today. Everybody knows those. Probably on the wealthy side. I thought it was interesting to look at Grace Hopper, the one in the middle. Was one of the people, one of the longest-serving Naval Officers we had, used to walk around with a 30 centimeter wire and say here's a nanosecond at the speed of light. She was one of the digital revolutionaries that we had. Absolutely superb.

The reason I really put this slide up is this. It goes back to where we started. When you look at what our nation has been able to do in cyberspace, it's extraordinary. We should be hugely proud

of what this represents. The hardware. The software. The social network capabilities and what this means for our futures.

You know, I have 13 grandchildren. Yeah, I know I'm not that old, I know, I know. But I have 13 grandchildren. The average age seems to be about three, two or three. They are already on the network. At 5, they are doing report… it's amazing what our children and our grandchildren will be able to do because of these capabilities. We're the nation that started the network. We're an innovation nation. We ought to be the nation that secures it.

So with that, I say go Rams! So thanks folks.